"Express Mail" mailing label number:

EV 335894656 US

SYSTEM AND METHOD FOR DETECTING COMPUTER PORT INACTIVITY

Brian A. Gonsalves
Kenneth R. Jones

Field of the Disclosure

[1001] The present disclosure relates generally to broadband communications, and particularly to a system and method for detecting an unattended or idle PC with an open data port.

Description of the Related Art

[1002] The widespread deployment of consumer broadband access, e.g., xDSL and/or cable modems, has benefited millions of subscribers by providing reliable, high speed Internet access. Broadband modems permit data downloads at speeds far above that obtainable through a conventional dial-up modem, e.g., 33 Kb/s or 56 Kb/s. However, as with many new technologies, there are also disadvantages associated with some aspects of the technology. For example, many broadband residential customers do not regularly update anti-virus software or employ firewalls/monitoring software on their broadband access computers. This leaves an unattended computer with a connection, or open port, to a wide area network. This open port is susceptible to probing and subsequent hijacking by malicious and/or unethical individuals, e.g., crackers and hackers.

[1003] A prominent recent case involving the use of zombies, or computers that are owned by third parties but taken over (hijacked) by crackers, was the Yahoo denial-of service (DoS) incident. In this incident, daemons (disk and execution monitors) were surreptitiously set up to generate spurious requests for information to Yahoo (and other sites such as Amazon, CNN, and eBay), at rates of up to one gigabyte per second, effectively shutting down Yahoo's equipment.

[1004] Subsequent investigations of the Yahoo DoS incident revealed that a majority of the owners of the computers that sent the spurious requests had broadband Internet access and were not even aware that their computers had been turned into zombies and used to carry out the DoS attack. Some people recalled noticing that their broadband connection seemed somewhat slower, but many people were not even at their computers during the times the attack was in progress.

[1005] Another troublesome recent development is the use of a virus sent to computer users to take over or hijack other people's computers to make them junk e-mail (spam) senders. Unlike most other mass-mailing viruses, this virus, dubbed AVF, doesn't e-mail itself to everyone in the infected computer's address book, but instead provides a backdoor into the computer. This backdoor is then utilized by spammers to send junk mail, providing anonymity for the spammers' illegal activities.

[1006] Scrupulous use of anti-virus software with regular updates and the use of personal firewalls and/or monitoring software could prevent the creation of zombie computers and hijacks. Turning off the unattended computer also provides protection. However, many people do not avail themselves of these options for various reasons ranging from lack of technical savvy to time constraints, or failing to understand the magnitude of the problem.

[1007] Accordingly, a need exists to provide additional security to unattended PCs with "always on" network connections.

SUMMARY

[1008] In a particular embodiment, a system for detecting an idle state in an end-user computer and subsequent blocking of the open Ethernet connection of the idle computer is presented. The system includes a first interface to a local area network (LAN) connection to an end-user computer and a second interface to a wide area network (WAN), such as a digital subscriber line (DSL) connection, to a distributed computer network, such as the Internet. In a particular embodiment, the second interface is coupled to an Internet service provider (ISP). Detection logic responsive to the first interface is used to detect user inactivity at the end-user computer, and blocking logic responsive to the detection logic selectively initiates a blocking signal to disable communications received from the second interface from being sent over the first interface to the remote end-user computer.

[1009] In a particular embodiment, the blocking logic sends the blocking signal in response to the detecting logic detecting the user inactivity for a selected period of time. In one embodiment, the selected period of time is between one and ten minutes. In another embodiment, the selected period of time is a fixed time period. In a further embodiment, the selected period of time is determined by a user of the end-user computer.

[1010] In a particular embodiment, the first interface, the detection logic, and the blocking logic are embedded within an auto-sensing Ethernet port. In another embodiment, the DSL connection carries authenticated point-to-point protocol over Ethernet (PPPoE) session traffic.

[1011] In a further embodiment, a method is disclosed that includes establishing a broadband connection, detecting an inactivity event, and blocking data. The broadband connection includes a first local data connection, e.g., an Ethernet connection, between an end-user computer and routing equipment, as well as a second, wide area data connection, e.g., a PPPoE session, between the routing equipment and an ISP. Detection of an inactivity event from the end-user computer occurs at the routing equipment, and is based upon detecting that the end-user computer has been idle for an idle time greater than an idle time activity threshold. The routing equipment then blocks data originating from the second, wide area data connection from being communicated to the first local data connection, thus establishing a blocking condition.

[1012] In another embodiment, the method further includes removing the blocking condition to allow communications from the second, wide area data connection to be sent to the first local data connection. Following blocking condition removal, data communications from the first local data connection is then allowed to be communicated to the second wide area data connection.

[1013] In a particular embodiment, a method of routing data at digital subscriber line (DSL) routing equipment is presented. The method includes establishing a first portion of a DSL connection and establishing a second portion of the DSL connection. The first portion of the DSL connection includes a local Ethernet data connection between an end-user computer and DSL routing equipment and terminates at a first port of the DSL routing equipment. The second portion of the DSL connection includes a wide area data connection between the DSL routing equipment and internet service provider (ISP) equipment and terminates at a second port of the DSL routing equipment. The method further includes detecting, at the first port of the DSL routing equipment, an indication that the end-user computer has been idle for an idle time greater than an idle time inactivity threshold. Further, during a first period of time, data received from the second port of the DSL routing equipment is blocked from being communicated by the first port of the DSL routing equipment.

[1014] In a particular embodiment, the method also includes, during a second period of time after the first period of time, detecting activity at the first port of the DSL routing equipment. This detection indicates activity at the end-user computer. In response to the activity detection, data received at the second port of the DSL routing equipment would be communicated to the first port of the DSL routing equipment, and to the end-user computer.

BRIEF DESCRIPTION OF THE DRAWINGS

[1015] **FIG. 1** is a general diagram illustrating a system for router/modem configuration to detect end-user computer inactivity and/or activity and to selectively block or unblock Ethernet port access accordingly; and

[1016] **FIG. 2** is a flow diagram illustrating methods for blocking and/or unblocking Ethernet port access to a personal computer.

DETAILED DESCRIPTION OF THE DRAWINGS

[1017] The present disclosure relates generally to broadband communications, and particularly to a system and methods for blocking external access, e.g., wide area network (WAN) access to an unattended or idle end-user personal computer (PC) with an open local area network (LAN) port. Employing the techniques disclosed herein provides an element of security to unattended PCs, and does not require end-users to install/configure additional hardware or software, thereby providing an element of convenience as well as connection security to end-users.

[1018] FIG. 1 is a general diagram illustrating a system for router/modem configuration to detect end-user computer inactivity and/or activity, as well as to selectively block or unblock Ethernet port access accordingly. The example system presented in FIG. 1 includes an end-user personal computer (PC) 104. The system also includes a first interface 108 to a local area network (LAN) Ethernet connection to the end-user computer 104 in communication with an auto sensing Ethernet port 120 in a router/modem 101. The router/modem 101 includes a second interface 110 to a wide area network (WAN) digital subscriber line (DSL) connection from a DSL port 124 to a distributed computer network 106. The distributed computer network 106 can be a public Internet protocol (IP) network, such as the Internet. The second interface 110 may be coupled to an Internet service provider (ISP). In a particular embodiment, the DSL connection of the second interface 110 carries authenticated point to point over Ethernet (PPPoE) session traffic.

[1019] The auto sensing Ethernet port 120 includes detection logic 130 responsive to the first interface 108 and is used to detect user inactivity at the end-user computer 104. The auto sensing Ethernet port 120 also includes blocking logic 132 responsive to the detection logic 130. Blocking logic 132 is used to selectively initiate a blocking signal to disable communications received from the second interface 110 from being sent over the first interface 108 to the end-user computer 104. In an exemplary embodiment, the detection logic 130 and the blocking logic 132 are embedded within the auto sensing

Ethernet port 120. In other embodiments, these elements may be separate components or may be integrated with other functions.

[1020] The blocking logic 132 sends a blocking signal in response to the detection logic 130 detecting user inactivity on PC 104 for a selected period of time. In a particular embodiment, the selected period of time is between one and ten minutes of inactivity, as detected by detection logic 130. In other embodiments, the selected period of time can be a fixed time period, which may be a default time period, e.g., five minutes, or the selected period of time may also be determined by a user of the end-user computer 104.

[1021] The router/modem 101 may be digital switching equipment such as a router or routing equipment, or may be a modem. The modem may be an asynchronous digital subscriber line (ADSL) modem, a digital subscriber line (DSL) modem, or other xDSL modems or high-speed interfaces utilized to establish layer 2 connections, e.g., PPPoE, between an ISP and the customers of the ISP.

[1022] FIG. 2 is a flow diagram illustrating methods for blocking and/or unblocking Ethernet port access to a personal computer. In step 202, a digital subscriber line (DSL) connection is established between an end-user computer to an Internet service provider (ISP). The DSL connection includes a first local data connection between an end-user computer, e.g., an Ethernet connection, and routing equipment and a second wide area network (WAN) data connection, e.g., a PPPoE session, between the routing equipment and the ISP.

[1023] Typically, both the first data connection and the second data connection are always open connections, however, this provides an "open door" for outside port scanners who may be looking for open connections to hijack. However, the present disclosure utilizes detection logic in the routing equipment, e.g., a router or modem, to detect that an end-user computer has been idle for an idle time greater than an idle time inactivity threshold to determine that an inactivity event has occurred at the routing equipment, as in step 204. The idle time inactivity threshold, or specified amount of time of inactivity by the end-user computer, can be a fixed threshold defining a fixed amount of time, or can be a programmable threshold. Further, a method for receiving user defined idle time information may be employed. This method would permit the modification of the idle time inactivity threshold to be set based upon the user's defined idle time information.

[1024] In response to detection of an inactivity event at the Ethernet port to the end-user computer and in response to blocking logic, the routing equipment 101 blocks all communication data originating from the second connection (i.e. the WAN connection) to the Ethernet connection (i.e. LAN connection to PC), as in step 206. This, in effect, closes the open Ethernet connection port, thus providing an element of security to the unattended end-user computer. Generally, a connection cannot be hijacked if it is not available, i.e., is not open.

[1025] Once a user returns to actively using the computer, the routing equipment detects the activity from the end-user computer and removes the blocking condition to allow communications from the WAN data connection to be sent to the Ethernet connection of the end-user computer via the routing equipment, as in step 208. This unblocking step also may include allowing data to be sent from the Ethernet connection of the end-user computer via the routing equipment to the WAN data connection of the ISP, since the end-user computer is no longer unattended. At this point, a normal DSL connection has been reestablished.

[1026] The system and methods described herein provides for a flexible implementation. Although the invention has been described using certain specific examples, it will be apparent to those skilled in the art that the invention is not limited to these few examples. Additionally, various types of routers, routing equipment, and/or modems are currently available which could be suitable for use in detecting and blocking idle connections for Ethernet communication sessions when employing the methods and system as taught herein. The above-disclosed subject matter is to be considered illustrative and not restrictive and the appended claims are intended to cover all such modifications, enhancements, and other embodiments which fall within the true spirit and scope of the present invention. Thus, to the maximum extent allowed by law, the scope of the present invention is to be determined by the broadest permissible interpretation of the following claims and their equivalents, and shall not be restricted or limited by the foregoing detailed description.